Vanaf 25 mei 2018 gelden er nieuwe regels voor de bescherming van persoonsgegevens. In dit artikel geven we uitleg over hoe je gegevens kunt beveiligen en wat je moet doen als je te maken krijgt met een datalek.

Reageer meteen op datalek

De beveiliging van persoonsgegevens begint al bij het beperken van het aantal gegevens dat je vastlegt. Hoe minder gegevens je bewaart, hoe kleiner het risico. Als financiële onderneming ben je op grond van de AVG verplicht, om voor de beveiliging van de persoonsgegevens passende organisatorische en technische maatregelen te treffen. Bij organisatorische maatregelen kun je denken aan het beveiligen van je fysieke dossiers en het beperken van toegang tot persoonsgegevens voor bepaalde medewerkers. Technische maatregelen zijn bijvoorbeeld versleuteling van gegevens, gebruik van unieke gebruikersnamen en wachtwoorden en het 'pseudonimiseren' van persoonsgegevens.

'Wft-gerelateerd incident aan AFM melden'

PASSEND NIVEAU

Er is sprake van een passend niveau van beveiligingsmaatregelen als je deze zodanig inricht, dat ze passen bij de gegevens die je verwerkt en de verwerkingen die je verricht. Denk daarbij bijvoorbeeld aan het verwerken van gevoelige persoonsgegevens. In die gevallen moet de beveiliging zwaarder zijn dan wanneer je geen gevoelige gegevens verwerkt.

Een datalek is een inbreuk op de beveiliging van gegevens waarbij persoonsgegevens verloren zijn gegaan, ongeoorloofd zijn gewijzigd, verstrekt, ingezien of toegankelijk gemaakt. Hiervan is bijvoorbeeld sprake als je gegevens per ongeluk naar de verkeerde afzender stuurt, een USB-stick verliest of als je systeem gehackt wordt.
Als je vermoedt dat er sprake is van een datalek, dan moet je direct onderzoeken of dat daadwerkelijk het geval is. Je legt daarbij vast wat voor soort datalek het betreft, wat de mogelijke gevolgen van het datalek zijn en welke maatregelen je hebt getroffen of nog gaat treffen.

MELDEN

Als er een datalek is geweest en de kans aanzienlijk is op ernstige nadelige gevolgen voor de bescherming van persoonsgegevens, dan moet je dat zonder vertraging melden aan de Autoriteit Persoonsgegevens. Indien mogelijk moet je binnen 72 uur een melding doen. Het is mogelijk dat je alvast een gedeeltelijke melding doet, bijvoorbeeld als het onderzoek wat langer duurt. De melding aan de Autoriteit Persoonsgegevens moet je doen via een standaardformulier dat beschikbaar is op de website van de toezichthouder.
Op grond van de Uitvoeringswet AVG is een melding van een datalek aan betrokkenen niet verplicht voor financiële ondernemingen, maar als er sprake is van een incident in de zin van de Wft dien je wel een melding aan de AFM te maken.
Voor de bescherming van persoonsgegevens is beveiliging van groot belang. Maar het is ook belangrijk dat je weet hoe je moet handelen als er onverhoopt sprake is van een datalek. Adfiz geeft haar leden hierover duidelijke uitleg. Waar nodig ondersteunt zij leden ook met praktische tips en tools. ■

Deze samenvatting wordt u aangeboden door Adfiz.